TASK ORDER (TO) 47QFCA21F0070

Awarded under Alliant 2 Contract 47QTCK18D0004

INTEGRATED MISSION, ANALYSIS, AND OPERATIONS (IMAX)
MISSION INFORMATION TECHNOLOGY (MIT)

in support of:

Defense Threat Reduction Agency (DTRA)

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

July 23, 2021

FEDSIM Project Number DE01111

C.1 BACKGROUND

The Defense Threat Reduction Agency (DTRA) is a combat support agency that enables the Department of Defense (DoD), U.S. Government, and international partners to counter and deter Weapons of Mass Destruction (WMD) and improvised threat networks. DTRA is the DoD's leader for targeted WMD and improvised threats, Research and Development (R&D), and it facilitates innovation to develop and quickly field solutions to the most complex, deadly, and urgent threats in the world. DTRA began strictly as a weapons development program in 1942 as part of the Manhattan Project called the Defense Special Weapons Agency; it expanded during the Cold War to eventually included non-nuclear weapons development and nonproliferation efforts. In November 1997, the Defense Reform Initiative merged the Defense Special Weapons Agency and the On-Site Inspection Agency with two defense programs – the Cooperative Threat Reduction (CTR) Program and the Chemical-Biological Defense Program, Science, and Technology component. These programs formed the core elements of DTRA.

DTRA was formally established on October 1, 1998. As threats continued to evolve, the DoD also established the Joint Improvised Explosive Device Defeat Organization (JIEDDO) in 2006 to lead and coordinate the DoD's Counter-Improvised Explosive Device (C-IED) efforts. Since 2006, the nature, scope, and use of improvised threat devices significantly evolved and increased in lethality and accessibility to the enemy. These threats now come from state actors, terrorist groups, enemy combatants, and widely divergent improvised threat networks.

In 2015, the Deputy Secretary of Defense expanded JIEDDO's mission from solely countering/defeating Improvised Explosive Devices (IEDs) to countering and defeating improvised threats at large. With this expanded mission, the name of the organization changed to the Joint Improvised Threat Defeat Organization (JIDO), and JIDO was ultimately re-aligned under DTRA in 2016. The JIDO functions have been fully integrated with DTRA, and the JIDO name has been retired.

In 2019, DTRA created the Integrated Mission, Analytics, and Operations (IMAX) acquisition strategy to integrate DTRA's intelligence, analytics, visualization, and operational support requirements into a focused and responsive capability to counter and deter WMD, improvised threats, and threat networks.

This TO provides supporting capability to the warfighter (Combatant Commands), as well as DTRA mission partners (e.g., all DoD agencies, military services, law enforcement agencies, Other Government Agencies).

C.1.1 PURPOSE

The purpose of this Mission Information Technology (IT) TO is to rapidly develop, implement and maintain DTRA Mission IT systems and capabilities, such as Catapult, Attack the Network Tools Suite (ANTS), Voltron, and other technology-based solutions to counter and deter WMD, improvised threats, and threat networks. The Mission IT TO enables rapid aggregation, fusion, and dissemination of operational information, intelligence, and technology to assist DTRA in countering and deterring WMDs, improvised threats, and threat networks in the Continental

United States (CONUS) and Outside the Continental United States (OCONUS). The TO provides custom-developed IT capabilities and operationalizes advanced technologies from public, private, and academic sectors. The TO provides the ability to innovate, adapt, and meet existing and emerging threats, while leveraging analytical Techniques, Tactics, and Procedures (TTPs) learned from embedded support to Combatant Commands (CCMDs) and tactical operations.

C.1.2 AGENCY MISSION

DTRA is a combat support agency that enables the DoD, U.S. Government, and international partners to counter and deter WMD and improvised threat networks. DTRA is the DoD's leader for targeted WMD and improvised threat R&D and facilitates innovation to develop and quickly field solutions to the most complex, deadly, and urgent threats in the world. DTRA's mission is three pronged:

a. To counter the threats posed by the full spectrum of WMD including Chemical, Biological, Radiological, Nuclear, and high-yield Explosives (CBRNE).

b. To counter threats posed by the growing, evolving categories of improvised threats including IEDs and car bombs as well as the tactics, technologies, and networks that put them on the battlefield.

c. To ensure the U.S. military maintains a safe, secure, effective, and credible nuclear weapon deterrent.

C.2 SCOPE

The IMAX MIT TO will provide direct IT services support to DTRA mission applications, systems, custom capabilities, supporting infrastructures, and other technology-based solutions in the CONUS and OCONUS. Under the IMAX MIT TO, the contractor shall provide custom-developed IT capabilities and operationalize advanced technologies from public, private, and academic sectors to support DTRA mission requirements. The TO will provide the ability to innovate and adapt capabilities, leveraging analytical Techniques, Tactics, and Procedures (TTPs) learned from embedded support to CCMDs and tactical operations. This TO includes, software development, data integration, system integration, direct operations, engineering, and Operations & Maintenance (O&M) support to mission applications, mission systems, and supporting infrastructure.

Note: DTRA is a Combat Support Agency (CSA), as described in C.1. DTRA is funded to support external mission partners as part of DTRA's core mission. References to mission partners do not imply contributed funding or performance of work external to DTRA's mission.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

Current capabilities and infrastructure descriptions are included in **Section J, Attachment E**.

C.4 OBJECTIVE

DTRA's mission benefits from continuous innovation enabled by effective program management, software development, system integration, direct operations, engineering, and

Operations & Maintenance (O&M) support to mission applications, mission systems, and supporting mission infrastructure. DTRA's support to mission partners is continuously modernized and improved through integration and delivery of advanced data solutions and technologies that leverage Commercial Open-Source Software (COSS), Commercial Off The Shelf (COTS), Government Off The Shelf (GOTS), Government Open Source Software (GOSS), advanced data methodologies, cloud services, Non-Developmental Items (NDI), and Non-Materiel Solutions in response to Government-approved mission requirements.

C.4.1 DESIRED OUTCOMES

Task 1 – Provide Program Management

a. TO performance is delivered at or above levels as provided in the Performance Requirements Summary (PRS)/Service Level Agreements (SLAs) for mission-support quality, cost, and schedule.

Task 2 – Provide Transition Support

a. DTRA support is sustained in a controlled and deliberate manner throughout transition with no degradation in capabilities.

Task 3 - Provide Mission Information Technology (IT) Capabilities Planning, Strategy, Software Development, and Systems Integration

a. Leveraging advanced technologies and development/delivery methodologies to meet emerging mission initiatives and requirements.
b. The analysis methods and requirements of Operations/Integration analysts, users, and mission partners are effectively incorporated into mission capability features and functions.
c. Mission IT capabilities are delivered on time, within budget, and without defects that require correction and re-work.

Task 4 - Mission Partner Outreach, Data, and Analytics Support

a. Innovative analytical capabilities are developed and delivered to internal and external DTRA customers in direct response to RFS and other mission requirements as they develop in real time.
b. Sharing of data, capabilities, and analytical methods is facilitated among DTRA organizations and DTRA's mission partners to maximize adoption and adaptation to current and emerging threats and priorities.
c. Capabilities are informed by analysis methods and insights from remote user environments.

d. Data can be shared in different ways from an organization allowing the ingestion of data into DTRA's mission IT system architecture to simplify granting access to data when ingestion is not feasible or desired.

e. Acquisition and integration of data and new data sources are continuously managed and improved. When acquisition of data is not available or feasible, but access is needed, innovative tools and (AI) generate innovative analytical methodologies and capabilities.

Task 5 – Mission Enclave Operations, Cybersecurity, Testing, Deployed IT, and Sustainment Support

a. The mission enclave technology support services enable delivery of mission capabilities to DTRA internal mission functions and external mission partners in compliance with emerging mission requirements, Government direction, and DoD and DTRA partner requirements.

b. Mission capabilities and the supporting infrastructure remain continuously compliant with DTRA, DoD, DISA, and IC cybersecurity and technical requirements.

C.5 TASKS

The following describes the services required for each Task. The contractor shall provide products and services in a timely and cost-effective manner and shall perform to or exceed the desired outcomes contained in the Performance Requirements Summary (PRS)/Service Level Agreements (SLAs) (**Section J, Attachment F**) and AFDP (**Section J, Attachment D**).

Task 1 – Provide Program Management

Task 2 – Provide Transition Support

Task 3 – Provide Mission Information Technology (IT) Capabilities Planning, Strategy, Software Development, and Systems Integration

Task 4 – Provide Mission Partner Outreach, Data, and Analytics Support

Task 5 – Provide Mission Enclave Operations, Cybersecurity, Testing, Deployed IT, and Sustainment Support

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall support Task 1 in accordance with the AQL as described in the PRS/SLAs (**Section J, Attachment F**).

C.5.1.1 SUBTASK 1.1 – ACCOUNTING FOR SERVICE CONTRACT REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for DTRA. The contractor shall completely fill in all required data fields using the following web address: http://sam.gov.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.sam.gov.

C.5.1.2 SUBTASK 1.2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at the location approved by the Government (**Section F, Deliverable 04**). The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the contractor's Key Personnel, representatives from the directorates, the DTRA Technical Point of Contact (TPOC), other relevant Government personnel, the FEDSIM CO, and the FEDSIM COR.

At least three days prior to the Project Kick-Off Meeting, the contractor shall provide a Project Kick-Off Meeting Agenda (**Section F, Deliverable 04**) for review and approval by the FEDSIM COR and the TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.
b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
c. Project Staffing Plan and status, to include Time Phase Labor Matrix (TPLM) (**Section F, Deliverable 02**).
d. Transition-In Plan (**Section F, Deliverable 01**) and discussion.
e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
f. Financial reporting and invoicing requirements.
g. Draft Project Management Plan, which contains an approach for providing and ensuring quality (**Section F, Deliverable 03**).

The Government will provide the contractor with the number of Government participants for the Project Kick-Off Meeting, and the contractor shall provide copies of the presentation for all present.

The contractor shall draft and provide a Project Kick-Off Meeting Minutes Report (**Section F, Deliverable 05**) documenting the Project Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 1.3 – PREPARE A TASK ORDER (TO) CONCEPT OF OPERATIONS (CONOPS)

The contractor shall deliver a TO CONOPS (**Section F, Deliverable 06**) for Government review and approval. The TO CONOPS shall reflect the contractor's:

a. Understanding of the DTRA mission and describe the contractor's approach to supporting the Government's execution of the DTRA mission.

b. Labor capacity management model and approach to providing mission IT support that rapidly adjusts and scales to support approved initiatives and additional as-needed requirements. The TO CONOPS shall describe the contractor's approach to supporting the DTRA CONOPS, emerging threat, and analytical problem sets.

c. Approach to inform mission IT activities through feedback, lessons learned, TTPs, and Area of Responsibility (AOR) insights from mission IT users, including deployed forces and intelligence analysts.

d. Approach to rotation of personnel across functions and teams such as data sciences, data integrators, innovation teams, and embedded support to improve mission knowledge and diversification of skill sets.

C.5.1.4 SUBTASK 1.4 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall deliver a Monthly Status Report (MSR) (**Section F, Deliverable 07 and Section J, Attachment J**). At a minimum, the MSR shall include the following:

a. Percentage of funding and ceiling expended, Estimates to Complete (ETCs) and Estimates at Completion (EACs) costs per CLIN for the current option period.
b. Projected funding exhaustion date per CLIN.
c. TO overview depicting trends for financial, schedule, staffing, and risks.
d. Executive-level summary of work accomplished by task area during the reporting period.
e. Actual travel costs for the month and planned travel costs for the following month.
f. A personnel roster in organizational chart format of individuals assigned to the TO and whether each is a Full-Time Equivalent (FTE) or a fraction of an FTE. Identify FTE count by task and provide a combined total for the TO.
g. SLA scorecard depicting monthly performance against Acceptable Quality Level (AQL) for each SLA.
h. Financial overview by CLIN and Task, and by funding source and appropriation type, including actual expenditures, accrued non-invoiced expenditures, and projected expenditures compared to funded and ceiling value.
i. Invoice (e.g., invoice number, invoice submittal date, amount, etc.) and payment history.
j. Cost, expenditure, and percentage of completion reporting for designated projects, efforts, and initiatives (i.e., tracking of projects designated by the DTRA TPOC or FEDSIM COR for separate project-level tracking)
k. Program issues, risks, and mitigations.
l. Actions required by the Government.

The contractor shall also deliver a monthly Labor CLIN(s) EAC Report that details total estimated labor cost per funding source through the end of the current period of performance (**Section F, Deliverable 08**).

Funding may include different appropriation types (e.g., O&M, Research, Development, Test, and Evaluation (RDT&E), Procurement, Defense-Wide (PDW), etc.) At the direction of the

DTRA TPOC or FEDSIM COR, the contractor shall account for and report expenditure of each funding source and each appropriation type to ensure that labor and non-labor expenditures adhere to DoD and DTRA financial management requirements. The contractor shall report each funding source and appropriation type as a separate line item under the appropriate CLIN in MSR financial reports and in the EAC deliverable.

C.5.1.5 SUBTASK 1.5 – PROVIDE INTEGRATED PROGRESS REVIEWS (IPRs)

The contractor shall present the MSR at a monthly IPR (**Section F, Deliverable 09**) meeting to the DTRA TPOC and the FEDSIM COR. The IPR shall be scheduled within five business days after MSR delivery, pending availability of Government personnel.

C.5.1.6 SUBTASK 1.6 – PREPARE PROJECT MANAGEMENT DOCUMENTATION

The contractor shall prepare and update, as requested, project management documentation (**Section F, Deliverable 10**) for efforts designated by the DTRA TPOC as IT projects. Project management documentation shall include the following:

a. A summary overview and project schedule updated and presented monthly, serving as a management dashboard identifying the project lead, short summary description, commit date, initial and revised projected completion dates, percentage complete, funding status, and priority.
b. A one-page “Quad Chart” (or other technical formats as approved by the DTRA TPOC) updated monthly for each designated project, including a short project description, overall status, risk statements including severity (impact and likelihood) and recommended mitigations, next actions, and scheduled milestone(s) status.
c. Project plans and schedules prepared and updated in Microsoft (MS) Project, or other formats/applications, with Work Breakdown Structures (WBS), milestones, schedules, or other information as appropriate for the project.
d. Monthly project status presentation to the DTRA TPOC and Task Lead(s), scheduled within five workdays of delivery of the Monthly Status Report, pending availability of Government personnel.
e. Revised staffing plans and cost estimates that capture changes in Level of Effort (LOE) resulting from evolving DTRA mission requirements and IT efficiencies.
f. To support DTRA planning and decision processes, the contractor shall deliver cost estimates, LOE estimates, staffing plans, project plans, technical approach documentation, and other decision support information. The contractor shall provide project-level tracking (e.g., funds expenditures, EAC, work completion, etc.) for project-based activities.

C.5.1.7 SUBTASK 1.7 – CONVENE, SUPPORT, AND PARTICIPATE IN PROJECT AND TECHNICAL MEETINGS

The contractor shall participate in TO-related management meetings, technical working groups, technical interchange meetings, and program management reviews, and shall support technical requirements review meetings throughout the period of performance in support of DTRA activities. Examples include non-recurring and recurring (on a daily, weekly, or monthly basis) stand-up meetings, IT leadership meetings, project and technical status briefings, requirements reviews, technical exchanges meetings with internal and external organizations, recurring briefings to Government leadership, and other briefings and meeting support as required.

The contractor shall be responsible for coordination of IT activities that cross DTRA organizations and for representation on integrated project teams to ensure that collaborative DTRA mission activities are properly supported. The contractor shall also develop Briefing/Presentation Materials, Reports, and Plans (**Section F, Deliverable 12**) and communicate TO status and issues to DTRA, FEDSIM, and other stakeholders as appropriate. Recurring technical reports shall include a monthly Mission IT System Metrics Report (**Section F, Deliverable 13**) that detail technical mission metrics directed by the DTRA TPOC. Metrics reporting includes the users, organizations, and ANTS tool usage breakdown by network, customer organization, or user group, or other metrics as directed by the DTRA TPOC when supportable by automation or other statistical collection methods. The contractor shall deliver a Lessons Learned Report (**Section F, Deliverable 14**). The contractor shall prepare a record of each meeting (**Section F, Deliverable 05**).

C.5.1.8 SUBTASK 1.8 – PREPARE COST ESTIMATES, TECHNICAL REPORTS, AND BRIEFINGS

The contractor shall prepare and update an SLA deliverable (**Section F, Deliverable 11**) document to augment the PRS/SLAs as directed by the Government. The SLA shall include details on the performance measures, AQLs, monitoring methods, and incentives/deterrents as indicated in the AFDP (**Section J, Attachment D**).

The contractor shall prepare cost estimates, technical reports, and briefings (**Section F, Deliverable 12**) related to issues generated during the performance of the requirements of the TO. These deliverables may be required to support DTRA leadership planning, programming, funding, and decision processes. Modification or re-baselining of previously approved cost estimates and/or technical reports will require Government re-approval.

The contractor shall develop and maintain a mission-system Lifecycle Management Plan (LCMP) (**Section F, Deliverable 15**). The Plan shall make recommendations for refresh of existing hardware, software, and systems and shall identify requirements for new systems and infrastructure upgrades, cost estimates, asset disposal, schedule/timing options, sourcing strategies.

C.5.1.9 SUBTASK 1.9 – PROVIDE MISSION INFORMATION TECHNOLOGY (IT) ACQUISITION TECHNICAL AND ACCOUNTABILITY SUPPORT

The contractor shall provide technical and administrative support for the purchase of mission IT hardware, software, and related infrastructure needs. The contractor shall develop and maintain comprehensive project cost estimates, projections, and IT Spend Plans (**Section F, Deliverable 12**). The contractor shall forecast and report planned purchases of hardware, software, and ODC services expenditures in reports that include purchases per option period, fiscal year, and fiscal-year quarter as directed by the DTRA TPOC (**Section F, Deliverable 12**).

Purchases of IT hardware, software, and specialized services will be made through approved contract processes as described in Section H. Contractor IT spend plans shall forecast and track new requirements, renewals, supplies, and other items as directed by the DTRA TPOC. Contractor IT spend plans, supporting technical specifications, and purchase requests shall be approved by the FEDSIM COR in coordination with the DTRA TPOC prior to initiating acquisition. The contractor shall follow DTRA Configuration Management (CM) procedures and coordinate with Government personnel as directed by the DTRA TPOC. The contractor shall coordinate delivery of equipment from suppliers to DTRA warehouse facilities and to the final installation site. The contractor shall comply with DTRA property accountability activities by ensuring that IT equipment is processed through the DTRA inventory accountability processes prior to being placed in service. For accountable IT equipment, the contractor shall report movement, replacement, and disposition to the Government hand-receipt holder.

C.5.1.10 SUBTASK 1.10 – IMPROVE TASK ORDER (TO) EFFICIENCIES AND EFFECTIVENESS

The contractor shall establish a continuous process improvement program with the objective of reducing costs while improving quality and mission effectiveness. Cost reductions that are accompanied with demonstrated quality improvements will be rewarded in accordance with a scheme proposed by the contractor (e.g., earned award fee) and approved by the Government in the PRS/SLA, AFDP, and award-fee activities.

The contractor shall identify and propose discrete Innovation Projects (IPs) for Government approval. Proposed IPs are not restricted to this TO (i.e. TO process touchpoints to other DTRA processes). Each IP shall include the following information as a minimum:

a. Estimated cost savings or cost avoidance.
b. Expected and measurable improvements to quality or mission effectiveness.
c. Timeline for implementation.
d. Government-provided material, information, assistance, and funding.

For each Government-approved IP, the contractor shall prepare and submit an Implementation Plan within 30 calendar days (**Section F, Deliverable 16**). The Government will prioritize the IPs and authorize a start date for each, pending execution of funding actions or investments required by the Government. The contractor shall track and report estimated and actual/realized cost savings or cost avoidance as well as realized quality and mission effectiveness changes (positive or negative) for each Government-approved IP.

C.5.1.11 SUBTASK 1.11 – CATAPULT PROGRAM SUPPORT

The contractor shall provide technical support to the Catapult Program Office and Government Catapult Program Manager, including preparation of technical documentation in support of DoD Instruction (DoDI) 5000.02, the Joint Capabilities Integration and Development System (JCIDS), and DTRA’s acquisition approval processes (**Section F, Deliverable 17**). This support can include technical working groups, technical interchange meetings, program management, and project reviews. For requirements within the scope of this TO, the contractor shall prepare and deliver briefings, white papers, and cost estimates, conduct research, and write technical documentation such as DoD Defense Architecture Framework artifacts, etc. The contractor shall support independent testing, third-party assessments, and Joint Interoperability Test Command

(JITC) interoperability testing for mission applications, systems, and development/delivery methodologies as required.

C.5.1.12 SUBTASK 1.12 – PREPARE TRIP REPORTS

The Government will require a Trip Report when the request for travel is submitted (**Section F, Deliverable 19**). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, Trip Reports shall be prepared with the information provided in **Section J, Attachment G**.

C.5.2 TASK 2 – PROVIDE TRANSITION SUPPORT

The contractor shall support Task 2 in accordance with the AQL as described in the PRS/SLAs (**Section J, Attachment F**). Transition-in shall begin immediately at time of TOA. Initial Operational Capability (IOC) is achieved on or before the Project Kick-Off meeting. Full Operational Capability (FOC) is achieved as soon as possible, but NLT 60 calendar days from TOA (with the exception of Task 5, as noted in table below). Transition-out is planned and managed effectively, support is sustained in a controlled and deliberate manner throughout transition with no degradation in capabilities.

IOC is defined as follows:

a. All required staffing to accomplish transition-in activities are in place.
b. The initial baseline TPLM, as specified in Section 5.1.2, has been submitted to the Government and required staffing in-processing activities are in progress.
c. Coordination efforts are established and synchronized with legacy contractors for their transition-out activities (facilitated by Government).
d. Contractor is in full control of transition-in activities.

FOC is defined as follows:

a. All tasks are fully staffed with fully qualified and trained personnel.
b. The contractor assumes full responsibility for management of all TO requirements.
c. All TO performance measures are fully accepted and are being reported.

. The contractor shall ensure a smooth and orderly transition-in to establish required support, and the contractor shall ensure all knowledge, data, material, and information developed by or provided to the contractor is transitioned and delivered to the Government by the end of the contract period.

The Government estimates the following IOC/FOC dates for transition-in below. The contractor shall ensure a smooth transition of support services with no degradation in capabilities during transition. The contractor shall plan for all contingencies from gradual to immediate staffing. NOTE: FOC date, for Task 5 is currently March 5, 2022, in Table 1 is a legacy contract expiration date. The Government reserves the right to accelerate FOC dates to meet evolving operational needs within 60 calendar days of Project Start, or for Task 5 within 60 days of Government indication.

Table 1. Full Operational Capability (FOC) Dates	
Task	**FOC Date**
Task 1 - Program Management	Project Start (PS) + 60 Days
Task 2 – Provide Transition Support	PS + 60 Days or start transition NLT 30 days before the dates shown in this table.
Task 3 – Provide Mission Information Technology (IT) Capabilities Planning, Strategy, Software Development, and Systems Integration	PS + 60 Days
Task 4 – Provide Mission Partner, Outreach, Data and Analytics Support	PS + 60 Days
Task 5 – Provide Mission Enclave Operations, Cybersecurity, Testing, Deployed IT, and Sustainment Support	March 5, 2022

C.5.2.1 SUBTASK 2.1 – TRANSITION-OUT

The contractor shall develop a Transition-Out Plan (**Section F, Deliverable 20**) for transitioning and delivering all material and information from this TO to the Government. The Plan shall identify all Government-Furnished Material (GFM) and Contractor-Furnished Material (CFM) as well as information and material developed during the TO that was used in the execution of this TO. The Transition-Out Plan shall be submitted for Government approval. Upon incorporation of comments and Government acceptance, the contractor shall follow the Plan to transfer all material, information, and rights thereto to the Government.

The contractor shall facilitate and conduct transition-out activities. The contractor shall update system descriptions and technical descriptions of all software, systems, and mission support activities delivered or performed under this TO. The contractor shall support transition of administrative and privileged access to the incoming contractor/Government, ensuring that no administrative access is lost. The contractor shall prepare a Final Contract Report documenting the status of all ongoing efforts and projects (**Section F, Deliverable 21**) and a Smartbook/turnover binder containing copies of all plans, policies, procedures, POCs, file storage locations for technical diagrams and documentation, and other information requested by the Government (**Section F, Deliverable 22**). Transition-out shall ensure no disruption to vital Government business. The contractor shall provide full cooperation in providing necessary operational knowledge to the incoming contractor.

Transition-out shall include the following types of services and information for knowledge transfer:

a. Project management processes.
b. Identification of POCs.
c. Location of technical and project management documentation, including Smartbook/turnover binders containing copies of all plans, policies, and procedures.

d. Status of ongoing technical initiatives and projects.
e. Incumbent contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel roles and responsibilities.
g. Identification of schedules and milestones.
h. Identification of actions required of the Government.
i. Establishment and maintenance of effective communication with the incoming contractor and Government personnel for the period of the transition via weekly status meetings.

The contractor shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor and/or Government personnel at the expiration of the TO.

The contractor shall implement its Transition-Out Plan NLT 60 calendar days prior to expiration of this TO.

C.5.3 TASK 3 – PROVIDE MIT CAPABILITIES PLANNING, STRATEGY, SOFTWARE DEVELOPMENT, AND SYSTEM INTEGRATION

The contractor shall support Task 3 in accordance with the AQL as described in the PRS/SLAs (**Section J, Attachment F**). Under this task, the contractor shall provide all MIT planning, strategy development, software development and system integration utilizing advanced technologies, development and delivery methodologies, across multiple software types (GOTS, COTS, COSS, GOSS, GSS, NDI, proofs of concepts) in order to support Government approved mission requirements for DTRA MIT stakeholders.

C.5.3.1 SUBTASK 3.1 – PROVIDE MISSION INFORMATION TECHNOLOGY (IT) ARCHITECT SUPPORT

The contractor shall provide subject matter expertise and serve as an advisor to DTRA leadership for activities within the scope of this TO including mission capabilities, ANTS, mission infrastructure, and support to the Catapult program (Ref. section H.1.2) The contractor shall prepare briefing materials (**Section F, Deliverable 12**), Product Demonstrations (**Section F, Deliverable 34**), DoD Architecture Framework Artifacts (**Section F, Deliverable 35**) and other technical materials as directed by the DTRA TPOC. Support may require local and non-local travel.

The contractor shall be responsible for:

a. The overall architecture of mission capabilities, Catapult, ANTS, and mission infrastructure.
b. Ensuring that mission IT capabilities and supporting infrastructure align with the DTRA mission and effectively address emerging threats and analytical problems.
c. Planning, strategy development, rationalization, and communication of an approved mission IT technical strategy.
d. Ensuring that big data analytic requirements and TTPs from users in DTRA, mission-partner, and deployed environments are identified to inform mission IT capabilities.
e. Leading special technology projects and research activities

f. Providing technical support to DTRA training missions, engagements, technical exchanges, product demonstrations, conferences, capability overviews, and briefings internally within DTRA and externally to DTRA partners.
g. Supporting meetings, delivering briefings, and providing demonstrations to Senior Executives and Flag Officers as required.
h. Providing technical advice and engineering guidance for next-generation planning efforts, including migration to or integration with other DoD or IC enterprise services, Government or commercial cloud environments.
i. Support the Catapult program office and Government Program Manager with technical advice, technical meeting support, architecture reviews, planning, and documentation.

C.5.3.2 SUBTASK 3.2 –MISSION INFORMATION TECHNOLOGY (IT) CAPABILITIES PLANNING

The contractor shall deliver a Software Development and System Integration Plan (SDSIP) (**Section F, Deliverable 23**) for Government review and approval. The SDSIP shall align with the DTRA's mission priorities and shall describe the contractor's methodology for delivering capabilities throughout the system lifecycle and at each step of the mission-capability path to production. The SDSIP shall identify Government-required review and approval gates at each phase of the path to production. The contractor's SDSIP shall provide for the ability to respond to quick reaction and expedited requests for support, within the scope of this TO, anywhere in the world and on a very short notice. For example, support may be in response to interruption in mission IT capabilities, requirements to provide direct technical support to deployed forces, assessment of mission needs and Tactics, Techniques, and Procedures (TTPs) in CONUS and OCONUS locations, emergency requirements for implementation of new or modified IT capabilities, or as-needed projects in response to new and emerging DTRA missions.

The SDSIP shall describe the contractor's approach, methodologies, steps, and process for delivering mission IT capabilities, including:

a. Software/System Development Lifecycle (SDLC) for on-premise, hybrid, and cloud-hosted path to production, as required by the Government, including scoping, requirements management, design, development, testing, installation support, maintenance, Tier-III support, and documentation. The SDSIP should provide for Tier III on-call support 24 hours per day, seven days per week (24x7) to address outages and incidents that degrade performance of mission applications and systems.
b. Continuous optimization of the existing mission capability path to production based on advanced methodologies including, but not limited to, implementation of Continuous Integration/Continuous Deployment (CI/CD), Secure Development Operations (DevSecOps), and automation of infrastructure and the pipeline of mission applications from development to production. Continuous optimization includes activities such as operating, maintaining, enhancing, and evolving DTRA's current mission-application DevSecOps instance, which includes automated code review, automated code testing, and automated security scanning to enable delivery of software through a fully automated pipeline from development to operations. CI/CD support also includes supporting other DTRA IT branches with software security and setting DevSecOps pipeline thresholds, policies, and procedures for the operation of the DevSecOps environment.

c. A methodology for expedited delivery of capabilities to meet mission requirements on or before a Government-approved Latest Time of Value (LTOV) date set by the requestor. LTOV delivery time frames may range from a few hours to days or weeks depending on real-world mission requirements. Expedited delivery provides the best possible capability within time and budget constraints, often in response to an urgent request by a DTRA mission partner or a warfighter.
d. An adopt/buy/create decision process for capabilities based on technical effectiveness (e.g. commercial, integration, academia, development, etc.).
e. A method for calculation of total cost of ownership and support analysis for O&M of mission IT capabilities in production environments (i.e., the O&M "tail").
f. A methodology for advanced technology prototyping and proof of concept efforts.
g. Source code management and version control processes, making maximum use of automated tools.
h. Software assurance, secure coding practices, automated software security analysis/scanning, and cyber-security compliance including technical analysis of security scan reports and support to remediation efforts.
i. Quality control and testing methodologies.
j. Processes that allow for collaboration with and technical support to other DTRA functions (e.g., mission IT operations, network engineering, CM, and cybersecurity) throughout the SDLC at each step of the path to production.
k. Expert recommendation for DTRAs strategy, which enable DTRA's mission as an early adopter of innovative technologies by acquiring, leveraging, and implementing advanced capabilities, methodologies, technologies, and subject matter expertise from public, private, and academic sectors that may be conceptual, experimental, or the product of DTRA and non-DTRA Research and Development (R&D) programs.

The contractor shall provide for planning functions in order to deliver Government-approved capabilities, which may be installed in DTRA and non-DTRA IT environments operated by the U.S. Government, allies, coalitions, and foreign partners. Classification levels of data, networks, and capabilities may include Unclassified, Secret, TS/SCI, and special access programs.

The contractor shall comply with DoD and intelligence community cybersecurity implementation guides, instructions, frameworks, and directives. Cybersecurity shall be integrated into the contractor's SDSIP (**Section F, Deliverable 23**). The contractor shall ensure that cybersecurity requirements are treated like other system requirements and are addressed early and continually throughout the software/system lifecycle in response to evolving threat, risk, compliance requirements, and mission.

The contractor shall deliver a Mission IT Baseline Assessment (**Section F, Deliverable 24**) for Government review and approval. This deliverable shall inventory and assess the DTRA mission IT baseline including existing mission IT software and systems, planned capabilities, and support requirements and make recommendations for modification, expansion, or obsolescence where needed.

The contractor shall prepare and deliver a Mission IT Roadmap (**Section F, Deliverable 25**). The Mission IT Roadmap shall provide a forward-looking plan for development and integration of mission capabilities and advanced technologies in alignment with current and emerging mission requirements.

C.5.3.3 SUBTASK 3.3 – MISSION INFORMATION TECHNOLOGY SOFTWARE DEVELOPMENT AND SYSTEM INTEGRATION

The contractor shall provide software development and systems integration activities utilizing advanced technologies and development/delivery methodologies to integrate capabilities to meet emerging threats. This includes support to provide proofs of concept, Commercial Open-Source Software (COSS), Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), Government Open-Source Software (GOSS), Non-Developmental Items (NDI), and Non-Materiel Solutions in response to Government-approved mission requirements originating from inside and outside of DTRA. The contractor shall maintain compliance with DTRA CM policies and procedures.

Specifically, the contractor shall provide the following:

a. Development, integration, and lifecycle support for DTRA mission IT capabilities including the Catapult big data analytic Framework and ANTS within DTRA local area networks (e.g., Unclassified, Secret, and Top Secret Sensitive Compartmented Information (TS-SCI)), on DoD and IC enterprise networks (e.g., Non-classified Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet), Joint Worldwide Intelligence Communications System (JWICS)), and other U.S. Government, allied, coalition, and special access networks as required.
b. Enhancement of mission applications and systems (e.g. Catapult, ANTS tools, other mission applications) to operate in Government cloud (existing DoD or IC) environments. This may include a full cloud migration and/or hybrid solution as deemed in the best interest of the Government from an operational and cost perspective.
c. Migration of existing mission applications and systems from on-premise hosting to Government cloud environments when suitable environments become available.
d. Development of mission applications and systems that leverage the infrastructure, platforms, and services of existing and emerging DoD, IC, and commercial (as approved) enterprise and cloud services (e.g., enterprise services, code repositories, etc.)
e. Collaboration, development, integration, testing, and lifecycle support to DTRA initiatives that integrate COTS products and services with GOTS products and DTRA capabilities, including acquiring commercial support for the effort.
f. Development of the full technology stack (i.e., all system components including platform for mission IT capabilities) and automated pipelines for delivery of big data mission capabilities to premise and in Government cloud hosting environments. Automated CI/CD and DevSecOps-enabled delivery may support DTRA requirements/use in non-DTRA environments.
g. Development of software and applications, web-parts, mobile code (per DTRA mobile-code and cybersecurity policy), and other capabilities IAW SDSIP to support big data analytics for structured and un-structured intelligence and operational reporting from data sources across the whole of government.

h. Delivery of expedited development, hot fixes, error corrections, patches, feature revisions, and upgrades in response to Government-approved requirements from within and outside DTRA, Requests for Support (RFS), and Joint Urgent Operational Needs (JUONs).
i. Obtain, report, and apply feedback and lessons learned from users in all DTRA operating environments including deployed and remote OCONUS operations.
j. Perform lifecycle maintenance (e.g., enhancements, revisions, patches, updates, fixes, etc.) and provide Tier III technical support to DTRA mission IT capabilities.
k. Integration and maintenance of ingest functionality for approved data sources for mission IT capabilities.
l. Collaborate with DTRA, Defense Information Systems Agency (DISA), and Defense Intelligence Agency (DIA) infrastructure personnel to support the design, implementation, and maintenance of on premise, remote site, and cloud-based back up and disaster recovery capabilities for maintaining mission IT capabilities. This support includes working with DTRA IT operations and networking engineers to manage and maintain Catapult, ANTS, and other mission capability disaster recovery systems at remote locations.

.

The contractor shall perform automated software code security analysis/scanning (e.g., SonarQube, Prisma, and other applications depending on code type/language) using Government-furnished software and provide Test and Analysis of Findings Reports (e.g., root cause, false positive, and remedial actions) (**Section F, Deliverable 26**) in support of DTRA Security Test and Evaluation (ST&E) and the Authorization and Assessment (A&A) activities.

The contractor shall support cybersecurity activities by providing technical analysis of software vulnerabilities and flaws in collaboration with DTRA's Security Controls Assessor (SCA), testers, and risk assessment activities. The contractor shall support cybersecurity remediation activities, including completion of Plan of Action and Milestone (POA&M) tasks for mission capabilities. The contractor shall comply with the direction of DTRA cybersecurity officials, including the Authorizing Official (AO), Security Controls Assessor (SCA), and Information Systems Security Manager (ISSM). The contractor shall support DTRA efforts to ensure continued cybersecurity compliance in the technical baselines, system security architecture, data flows, and design of mission IT capabilities.

The contractor shall leverage or develop an Automated Dashboard Tracker (**Section F, Deliverable 27**) which includes effective measures and methodology of reporting agile development artifacts to the Government (e.g., labor capacity, requirements, backlog, burn-down rates, work in progress, projected completion dates)- Note: Atlassian JIRA software is currently in use. The contractor shall support DTRA efforts to measure and improve the mission IT path to production by tracking and reporting development and integration efforts from inception to installation in the production environment as directed by the Government. The contractor shall track and report user adoption rates for mission IT capabilities. The contractor shall maintain an automated capability or dashboard that tracks and reports mission IT usage statistics directly to Government personnel. The contractor shall support the operation and customization of other current JIRA-based applications in use by DTRA as directed by the DTRA TPOC.

The contractor shall deliver to the Government all designs, system descriptions, test plans, source code, and documentation (**Section F, Deliverable 28**) and other technical materials without proprietary information, restrictions, or markings unless approved in advance by the FEDSIM COR. The contractor shall provide software code commenting and descriptions sufficient to ensure continuity of support and continued maintainability.

The contractor shall support internal and external stakeholders by capturing, scoping, and validating mission and operational requirements and shall document these activities. (**Section F, Deliverable 12**). For new applications, systems, and major upgrades, the contractor shall prepare and update System/Application Description Documents (SDD) (**Section F, Deliverable 29**), as directed, that describe requirements, design, components, and functionality for mission IT capabilities. The contractor shall maintain version description documentation and release notes for inclusion in the SDD, installation guides, and other documentation as appropriate for each new release or revision. This information may be captured in a CM system ticket for minor releases and updates. The contractor shall maintain the SDD (**Section F, Deliverable 29**) in compliance with DTRA CM processes and in compliance with DoD and IC cybersecurity controls and requirements.

The contractor shall develop a Master Test Plan (MTP) (**Section F, Deliverable 30**) that describes all aspects of the contractor's test methodologies for Government approval. The contractor shall document test results in Test and Analysis of Findings Reports (**Section F, Deliverable 26**), using automated reporting methods where feasible. The MTP shall identify the contractor's approach to software and system quality, and test methodologies applied throughout the lifecycle including, where appropriate, unit testing, regression testing, functional testing, compatibility, interoperability testing, and other testing as required. These shall be accomplished using automated code security testing and scanning tools into development processes wherever feasible.

The contractor shall prepare and update Installation Guides (**Section F, Deliverable 31**) to guide system administrators and independent testers through the process of installing software and systems in the target environments.

The contractor shall prepare User Guides (**Section F, Deliverable 32**) in electronic and/or printable format to assist cybersecurity testers, administrators, DTRA Configuration Management (CM), and end users with mission IT capability uses, features, and functionality.

The contractor shall prepare and submit Change Requests (CRs) (**Section F, Deliverable 33**) in compliance with DTRA CM processes and procedures to authorize changes to mission systems and applications. CRs shall be opened at initiation of development and integration activities to enable measurement of the full path to production.

C.5.3.4 SUBTASK 3.4 – SUPPORT EXTERNAL COLLABORATION

In support of Task 3 requirements, the contractor shall provide technical support, appropriate to the role of a contractor, to external mission IT collaboration activities when directed by the FEDSIM COR to support DTRA Government meetings. The contractor shall provide subject-matter expertise within the scope of this TO to DTRA's inter-agency collaboration with and among the DoD, IC, U.S. Government Agencies, and U.S. allies and partners. The contractor shall support efforts to identify and implement big data mission IT capabilities that address the problem sets of U. S. Government agencies and mission partners. This shall include requirements definition, design, development, integration, prototyping, testing, and production support of mission IT and analytical capabilities within the scope of this TO. Support may include assisting in development of Memorandums of Agreement (MoAs), Memorandums of Understanding (MoUs), and other agreements. The contractor shall provide technical support to DTRA tiger teams and strategic outreach initiatives to U.S. Government agencies, allies, and partners.

The contractor shall participate in and provide technical support to technical exchange meetings, synchronization meetings, technology demonstrations, leadership briefings, status meetings, conference presentations, and other meetings and events. The contractor shall support collaboration among DTRA, the private sector, and academic sector organizations. The contractor shall prepare briefing slides, capability description materials, informational papers, mission IT capability descriptions, and other meeting support materials (**Section F, Deliverable 12**). The contractor shall prepare Meeting Minutes and After Action Reports (AARs) (**Section F, Deliverable 05**).

C.5.4 TASK 4 – PROVIDE MISSION PARTNER OUTREACH, DATA AND ANALYTICS SUPPORT

The contractor shall support Task 4 in accordance with the AQL as described in the PRS/SLAs (**Section J, Attachment F**). The contractor shall develop innovative analytical capabilities in direct response to mission requirements. The contractor shall develop an Integration and Operations Plan (**Section F, Deliverable 36**) for Government review and approval. This Plan shall describe the contractor's approach to executing direct operations support activities in alignment with the DTRA mission. This plan shall describe the contractor's methods to foster collaboration and knowledge sharing among the contractor's personnel within this TO, mission-partner personnel, and DTRA personnel (e.g., DTRA technologists and leadership, and DTRA operations/integration analysts). The contractor shall identify a methodology for rotation of personnel, where feasible, among TO positions to improve team dynamics, knowledge sharing, collaboration, and skillset diversification. This Plan shall describe the contractor's methodology of assessing and engaging each mission partner to identify unique mission requirements for delivery of customized mission support.

The contractor shall ensure that sharing of data, capabilities, and analytical methods are effectively facilitated among DTRA organizations and DTRA's mission partners to maximize adoption and adaptation to current and emerging threats and priorities; this includes utilizing applied data sciences, Machine Learning (ML) and Artificial Intelligence (AI). The contractor shall support this task by providing ML and AI analytics, producing analytical products, and providing subject matter expertise.

C.5.4.1 SUBTASK 4.1 - PROVIDE DIRECT OPERATIONS SUPPORT AND RAPID INNOVATION SUPPORT

The contractor shall identify customer requirements, problem sets, capability gaps, and unique tactical requirements. The contractor shall conduct rapid (as defined by the LTOV, a few hours to days or weeks depending on mission need) prototyping of analytical, visualization, modelling, and simulation capabilities in direct response to CCMDs, deployed forces, and other end users in operational environments. Innovations are informed by knowledge of analytical methods and through collaboration with analysts and other users who may be operating in theater, combat zones, or forward-deployed environments. The contractor shall identify and apply new technologies and methods as technology evolves and new capabilities emerge in commercial, public, and academic sectors to meet requirements. Capabilities may be required in a reach-back capacity to support users operating in potentially bandwidth-constrained environments.

The contractor shall deliver capabilities using three delivery models, as required: 1) transactional response to customer requirements (i.e., one-time responses to an RFS), 2) continuous support delivering multiple products and capabilities to ongoing customer requirement, and 3) rapid prototyping to develop, test, authorize, and field quick-reaction capabilities. The contractor, as the SME, shall identify and recommend advanced tools and software to deliver direct support and rapid innovation to deliver customer requirements. The contractor shall develop capabilities to include, but not limited to the following:

a. **Terrain Analysis** – Provide view-shed analysis, path planning, and operations visualization. The contractor shall support vulnerability assessments and other capabilities to assist deployed forces to optimize sensor placement in theatre areas of operation.
b. **Three-Dimensional (3D) Scene Visualization** – Create 3D models to support training, force protection, and operations planning and rehearsals. Models may include areas of named interest (cities, villages, supply routes, rivers) in theater using Light Detection and Ranging (LIDAR) when available, Digital Terrain Elevation Data (DTED), and national or commercial imagery as requested by DTRA customers. Models may be produced in lightweight format to support warfighters down range in bandwidth-constrained environments (e.g., Keyhole Markup Language Zipped (KMZ), 3D Portable Document Format (3DPDF), Vantage). Additionally, these 3D models shall be integrated with a support virtual reality usage (e.g., Oculus Rift, MS Holo Lens)
c. **3D Dashboard Application** – Develop 3D dashboard software to allow the warfighter to manipulate 3D models to add operational graphics, import shape files from GeoBrowser and other applications, create fly-through movies, and support counter-improvised-threat analysis in new novel manners.
d. **Mission Planning/Force Protection Simulations** – Provide mission planning/force protection modeling and simulation expertise, training, and software support. Mission planning and force protection shall include analysis of red and blue TTPs, sensors, new/modified military apparatus, blast modeling, vulnerability assessments, and first-person shooter scenarios. First-person shooter scenarios require development of software using gaming engines. Blast modeling products such as High Explosive Damage Assessment Model (HEXDAM) and Vulnerability Assessment and Protection Option (VAPO) are currently used for modeling blast effects. The contractor shall also provide scenario development and training for DTRA teams. Mission planning and force protection tools will also include capabilities to support and visualize Unmanned Aerial Systems (UAS) ranges and capabilities as well as counter-UAS capabilities and ranges.
e. **Modeling and Simulation Operations Analysis** – Provide research and analysis teams to evaluate new tools and techniques for modeling and simulation of emerging battlefield threats and enemy capabilities. The contractor shall provide blast/explosive simulations

for terrain and material construction. This analysis shall include detailed estimations and visualization of effects to personnel and structures in the event of explosive detonation.

f. **Analytic Innovation** – Collaborate with the Government to identify critical analytical and emerging-threat challenges and shall define and execute experiments and proofs of concept to demonstrate innovative capabilities to address the challenges. The contractor shall support capability maturation and operational implementation of successful efforts.

C.5.4.2 SUBTASK 4.2 - PROVIDE DIRECT SUPPORT TO DTRA MISSION PARTNERS

Direct support bridges the gap between DTRA and DTRA's mission partners to connect them to DTRA data, tools, and expertise. Direct support personnel facilitate adoption of DTRA capabilities in partner organizations and facilitate incorporation of mission partner data and expertise back into DTRA solution sets. The contractor shall provide Mission IT support to DTRA mission partners and serve as liaison (i.e. do not support mission partner requirements outside of the scope of DTRA requirements) and Mission IT SMEs to DTRA mission partners including U.S. Government agencies, CCMDs, Theater Special Operations Commands (TSOCs), and deployed units. The contractor shall provide support at DTRA facilities and partner facilities through permanent duty, local and long-distance travel, and temporary duty to locations worldwide in support of DTRA initiatives and decisive efforts.

C.5.4.2.1 SUBTASK 4.2.1 - PROVIDE ON-SITE SUPPORT TO MISSION-PARTNERS

The contractor shall provide local, on-site mission IT capability and data integration support to DTRA mission partners related to any tasks within the scope of this TO. The on-site representative serves as SME for integration of DTRA capabilities into each partner's mission and as a specialist in harvesting and operationalizing multi-intelligence data. Mission partner support may include:

a. Establishing liaisons and coordinating between DTRA and mission-partner personnel.
b. Identifying, coordinating, harvesting, and exposing relevant mission-partner data sources across multiple domains and classification levels for ingestion into DTRA mission IT capabilities, or the granting of access to data when not feasible to ingest to develop tools.
c. Identifying mission-partner priorities and problem sets in order to identify support gaps.
d. Gathering input and requirements for methodology development, tool modification, and tailored mission support.
e. Providing on-site assistance, instruction, and education to partner-site personnel to enable use of DTRA capabilities.
f. Collaborating with DTRA capability developers and data scientists to enable customization of mission IT capability features and functionality to meet mission-partner requirements.
g. Applying knowledge of mission-partner AORs, TTPs, operations, and mission priorities to ensure effective augmentation of DTRA data capabilities.
h. Enabling a robust community of users by facilitating sharing of analysis methods and mission IT use cases between partner-site personnel, DTRA analysts, and personnel at other partner sites.

i. Fostering collaboration among mission partners by establishing a POC and coordination point for communities of interest.
j. Facilitating collaboration and sharing of data, threat information, and analysis between DTRA and the mission partners.
k. Promoting visibility of DTRA capabilities by supporting collaboration events such as technical exchanges, conferences, and seminars among DTRA and the mission partners.
l. Identifying partner requirements for capability training and delivering training or leveraging DTRA training capabilities to meet requirements.
m. Drafting agreements and tailoring documentation (**Section F, Deliverable 39**) to support adoption and use of DTRA mission IT capabilities at the partner site.

C.5.4.2.2 SUBTASK 4.2.2 - PROVIDE MISSION INFORMATION TECHNOLOGY (IT) INTEGRATION SUPPORT

The contractor shall assist, support, and coordinate the integration of mission IT capabilities into mission-partner IT environments. Activities include identifying technical requirements, coordinating and providing technical support to enable remote access to mission IT, and facilitating adoption and use of DTRA mission IT capabilities by mission partners. The contractor shall identify partner-site IT infrastructure, technology, cybersecurity requirements, and procedures to enable the access, installation (where required), connection, approval and use of DTRA capabilities.

C.5.4.2.3 SUBTASK 4.2.3 - PROVIDE MISSION INFORMATION TECHNOLOGY (IT) INNOVATION SUPPORT

The contractor shall serve as an SME on mission-partner operations (e.g., mission priorities, threat-network analysis, operations/integration workflow analysis methodologies and TTPs, etc.). The contractor shall identify mission-partner problem sets, questions, technical challenges, workflows, and urgent needs that can be addressed by DTRA mission IT. The contractor shall combine knowledge of mission partner analytical methods and DTRA mission IT capabilities to identify new or modified solutions in support of the mission partner. The contractor shall organize focused teams of technologists, analysts, and other personnel to address specialized problem sets or unique mission requirements.

C.5.4.2.4 SUBTASK 4.2.4 - PROVIDE MISSION INFORMATION TECHNOLOGY (IT) TRAINING, SYMPOSIUMS

The contractor shall provide technical support and subject matter expertise to DTRA Government outreach activities such as conferences, technical exchange meetings, and collaboration events among DTRA and DTRA mission partners. In support of Task 4, the contractor shall develop and deliver demonstrations, on-site capability training, briefings, and operational assistance, and shall support training functions for mission IT capabilities (**Section F, Deliverable 40**). This support may require local and long-distance travel.

C.5.4.3 SUBTASK 4.3 - PROVIDE DATA ENABLED APPLIED ANALYTICAL SUPPORT

C.5.4.3.1 SUBTASK 4.3.1 - PROVIDE DATA SCIENCES AND LIFECYCLE DATA MANAGEMENT

The contractor shall provide data-source, data-integration, and data sciences support to enable applied analytical capabilities. The contractor shall define a methodology and continuously improve the acquisition and integration of data sources for ingestion into mission IT capabilities. The contractor shall identify data sources and provide advice, guidance, tracking, reporting, and technical solutions for ingestion of formal, tactical reporting sensor, and other structured and unstructured data sources into mission IT capabilities to satisfy requirements from DTRA and DTRA mission partners. The contractor's recommendations and technical solutions shall be informed by DTRA operations/integration analytical TTPs, mission-partner intelligence analysis expertise, lessons learned, and TTPs from tactical environments and deployed forces. The contractor shall report data-source integration schedule, status, and other data-source information, as directed by the DTRA TPOC, and shall support status meetings and decision processes.

The contractor shall provide data sciences support to enable processing of structured and unstructured data to derive patterns, trends, and correlations and to enable entity extraction, disambiguation, Common Operating Picture (COP)/Common Intelligence Picture (CIP) solutions, visualization, and other data-related support. The contractor shall identify analytical problem sets, emerging threat trends, and DTRA customer requirements for improved capabilities and shall apply data sciences skill sets to solve problems and satisfy requirements. Data sciences shall be applied to multi-intelligence, counter-improvised threat data feeds and repositories to enable query-driven analytics and dynamic, real-time reporting and visualization in response to changing threat, data sources, and DTRA mission requirements. The contractor shall provide data sciences support including, for example, entity extraction, entity resolution, pattern extraction, link analysis, human and social-network links/connections, data frameworks, visualization support, and related algorithms. The contractor shall support and operate a machine learning and artificial intelligence environment to include development of machine learning training sets, development of supervised and unsupervised training models, as well as the operationalization of data science models into existing and new big data applications, tools, and visualizations.

The contractor shall define and apply a methodology for data mapping and Extract, Transform, Load (ETL) services and to address changing enhanced data integration strategies. The contractor shall develop tools for importing data from disparate defense component databases and other structured and unstructured sources to ensure data feed utility and compatibility with mission IT capabilities as well as for providing a service layer to other agencies. The contractor shall provide technical advice on mission IT architectural transformations to accommodate data-ingestion requirements.

The contractor shall provide data lifecycle management and metrics reporting, including monitoring data sources, ingested data, and interfaces to determine their usage, mission relevance, and recommendations for deprecation or obsolescence, or replacement with different data sources. The contractor shall maintain documentation that supports the operational interfacing and the processes that are a part of mission IT systems, tools, and applications. This includes development of a Mission Data Model across the various environments (**Section F, Deliverable 37**) and development and maintenance of procedures associated with data interfacing, ingestion, migration, data cleansing, deprecation, etc. (**Section F, Deliverable 38**). The contractor shall ensure and monitor data ingestion, processing, handling, and retention for compliance with intelligence oversight instructions and procedures as defined in DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, DoD Manual 5240.1, Procedures Governing the Conduct of DoD Intelligence Activities, and DoD Directive 5148.13, Intelligence Oversight.

C.5.4.3.2 SUBTASK 4.3.2 - DEVELOP AGREEMENTS WITH EXTERNAL DATA SUPPLIERS

The contractor shall provide technical expertise to support DTRA efforts to develop agreements with mission partners to support data ingestion.

These agreements detail technical specifics to support data exchanges. This support shall include the development of draft agreements, technical specifications, data exchange methods and protocols, data exchange schedules, roles, responsibilities, and other information necessary to specify the inter-agency relationship and supply of data for ingest into mission IT capabilities.

C.5.5 TASK 5 – PROVIDE MISSION ENCLAVE OPERATIONS, CYBERSECURITY, TESTING, DEPLOYED IT AND SUSTAINMENT SUPPORT

The contractor shall support Task 5 in accordance with the AQL as described in the PRS/SLAs (**Section J, Attachment F**). The contractor shall provide support at the mission enclave at DTRA's Reston site. DTRA's Reston mission enclave is secure, compliant, and available to authorized users 24 hours per day, seven days per week (24x7). The contractor shall ensure that the CI/CD pipeline from development to production including automation, tools, and methodologies is continuously optimized to accelerate delivery of capabilities to users and mission partners. The contractor shall ensure that deployed capabilities are integrated, delivered, and supported to meet the mission, functional and schedule requirements of deployed forces. The contractor shall ensure mission capabilities and the supporting infrastructure remain continuously compliant with DTRA, DoD, DISA, and IC cybersecurity and technical requirements.

C.5.5.1 SUBTASK 5.1 – MISSION ENCLAVE ENGINEERING SUPPORT

The contractor shall improve mission system and infrastructure efficiency and effectiveness through engineering support services. These services support the enclave, and shall include, but are not limited to:

a. Engineering services to support infrastructure-related architecture and security protocols.
b. Optimizing DTRA's mission infrastructure to ensure alignment with DTRA mission priorities.
c. Implementation of applications, systems, and technologies to support DevSecOps enabled CI/CD automated pipelines.
d. Engineering and re-engineering infrastructure due to DTRA reorganization.
e. Replicating, migrating, transitioning, or decommissioning DTRA Mission IT

capabilities, data, and network services to other locations or domains as required.

f. Designing and engineering of DTRA's mission infrastructure to eliminate single points of failure, to optimize quality of service, and to maximize availability of capabilities to DTRA internal and external users.

g. Engineering IT architecture for mission system Disaster Recovery (DR), fail-over solutions, Continuity of Operations (COOP), and service availability.

h. Supporting special technology projects (e.g., advanced technology evaluations, proofs of concept, implementation planning), as required.

i. Providing technical infrastructure support to DTRA technical exchanges, product demonstrations, engagement events, capability overviews, and briefings internally within DTRA and externally to DTRA partners.

j. Planning and implementing transition from internally hosted IT services and mission capabilities to DISA, DTRA, or IC enterprise services or hosting sites as directed by the DTRA TPOC.

k. Design, engineer, and support data replication to local and remote DR systems.

l. Planning, piloting, and/or implementing mission capabilities and transition to enterprise services and virtualized and cloud-based technologies. DTRA is continually assessing options to transition IT services to cloud-based solutions in compliance with DoD mandates, DTRA transition activities, or to achieve performance efficiencies and improvements. DTRA requires the contractor to support internally hosted advanced technologies and to support Government decision to transition to DoD and IC enterprise and cloud services.

m. Making recommendations innovations and improvements in DTRA's mission enclaves that may result in increased efficiency, improved services, and/or reduced costs to the Government.

n. Providing the following technical reports as requested by the Government regarding the current and projected health of the DTRA IT infrastructure:

   1. Plans and procedures for anticipated events such as power outages, weather events, organizational changes, and data calls from DTRA leadership (**Section F, Deliverable 12**).
   2. Trend analysis, incident reports, problem reports, and outage notifications (**Section F, Deliverable 41**).
   3. Recommendations, technical proposals, technology roadmaps, and concept planning for improvements and changes for the mission enclave (**Section F, Deliverable 12**).
   4. Mission Infrastructure Descriptive Documentation (**Section F, Deliverable 42**) that documents and summarizes the architecture, topology, connectivity, and device composition and count of DTRA's infrastructure.

C.5.5.1.1 SUBTASK 5.1.1 – CONTINUITY OF OPERATIONS (COOP) AND DISASTER RECOVERY (DR) SUPPORT

The contractor shall provide IT support to DTRA COOP, DR, and fail-over efforts and site(s), primarily performing administration and coordination from the primary site. Currently, DTRA's primary mission support hosting site is located in Reston, Virginia. DTRA also operates a remote data DR hosting system in Northern Virginia and a failover system for mission IT systems in a remote western U.S. location. Local and long-distance travel to remote sites may be required periodically to perform site surveys, hardware installations, upgrades, and remote-site duties during activation of DR capabilities (when directed by the Government).

The contractor shall support the following DR-related activities:

a. Provide technical support to DTRA DR meetings.
b. Perform technical assessments and site surveys for DR sites and hosting services in support of DTRA planning activities.
c. Produce written plans, designs, surveys, and briefings (**Section F, Deliverable 12**) to assist DTRA in developing and documenting DR capabilities.
d. Provide IT technical liaison and coordination with DR facility service providers and managers.
e. Support and administer network connectivity, cryptography, circuits, and other communications systems between primary and remote facilities.
f. Provide IT-related technical support to the operation of DTRA DR capabilities.
g. Support implementation, configuration, and administration of mission DR systems (virtual and/or physical) that fall within DTRA's IT management control, authorization boundaries, and/or operate as an extension of the DTRA enterprise.
h. Exercise DR systems and infrastructure periodically to ensure that safeguards, backups, end-user services, and procedures can provide mission continuity in case of events such as primary-site loss, natural disasters, and power outages.
i. Support successful recovery of services after primary-site restoration or the establishment of alternate facility.

The contractor shall support the following COOP-related activities:

a. Provide IT-related technical input to DTRA COOP planning, design, and implementation efforts, including meeting and briefing support.
b. Provide IT-related technical liaison, coordination, and Tier I/II support with COOP facility service providers.
c. Support and administer network connectivity, cryptography, circuits, and other communications systems between DTRA and COOP facilities.
d. Support implementation, configuration, and O&M of DTRA Mission IT COOP assets that fall within DTRA's management control, security boundaries, and/or operate as an extension of DTRA mission systems.
e. Exercise mission-related COOP systems and infrastructure periodically to ensure that safeguards, backups, end-user services, and procedures can provide mission continuity in case of events such as primary site loss, natural disasters, and power outages.
f. Support successful recovery of services after primary site restoration or the establishment of an alternate facility.

C.5.5.1.2 SUBTASK 5.1.2 – PROOF OF CONCEPT, PROTOTYPING, AND PERFORMANCE OPTIMIZATION OF MISSION TECHNOLOGIES

The contractor shall support the DTRA mission as an early adopter of innovative technologies and mission capabilities by acquiring, leveraging, and implementing advanced capabilities, methodologies, technologies, and subject matter expertise from public, commercial, and academic sectors that may be conceptual, experimental, or the product of DTRA and non-DTRA development programs. The contractor shall advise Government personnel of relevant new or emerging technologies, perform technology assessments, and provide performance-enhancing recommendations as requested by the Government. Examples include delivery of new mission IT capabilities, responses to mission partner requests for support, and future alignment of DTRA's mission enclave infrastructure with DoD, IC, or DTRA enterprises.

The contractor shall continuously assess and optimize performance of the mission enclave, including the path and process by which mission capabilities are introduced into production environments. In collaboration with other DTRA organizations, the contractor shall optimize and automate the mission IT capability path to production to accelerate response to mission requirements and delivery of new capabilities. For example, the contractor shall implement and provide O&M of DevSecOps-enabled technologies and capability delivery methodologies.

The deliverables required for this work may take many forms such as information papers, service catalogues, IT roadmaps, process and procedure documentation, briefings, training packages, and CONOPS (**Section F, Deliverable 6 and Section F, Deliverable 12**).

C.5.5.2 SUBTASK 5.2 – PROVIDE MISSION ENCLAVE OPERATIONS AND MAINTENANCE (O&M)

The contractor shall perform the following work for all DTRA IT infrastructure and systems as directed by the Government:

a. Provide installation, configuration, administration, O&M, and operational availability support to DTRA mission IT capabilities (e.g., hardware, software, platforms, and connectivity) in development, testing, staging, and production environments.
b. Store, back-up, restore, and archive mission data on all servers and perform recovery operations as needed.
c. Maintain and optimize standard configurations, images, and system baselines on all mission enclave components.
d. Maintain and administer mission infrastructure management tools, including, but not limited to, Solarwinds, MS System Center Configuration Manager (SCCM), System Center Operations Manager (SCOM), Splunk, and CoreLight.
e. Maintain and operate network and system management software, and other systems such as patch servers, update servers, and storage solutions.
f. Manage on- and off-premise mission data storage systems.
g. Provide infrastructure O&M for data feeds and data ingest into mission IT applications and systems.
h. Create and maintain current, written Administrative and System Maintenance Procedures (**Section F, Deliverable 43**).

i. Perform acceptance testing to determine suitability of systems and software for operation in the production environment and follow DTRA's change management procedures to obtain Government approval to introduce new and modified mission capabilities, features, and updates into DTRA production environments.
j. Implement cybersecurity corrective actions, patches, bug fixes, and other remediation activities per POA&M and other requirements to maintain cybersecurity compliance.
k. Develop, update, and maintain technical documentation, user guides and "how to" materials to assist mission system users (**Section F, Deliverable 32**).
l. Install, implement, and integrate systems hosted for third-party organizations in accordance with site licensing agreement, interagency agreements, or as requested by the Government.
m. Administer and maintain DTRA's implementations of workflow automation solutions that currently include BMC Remedy and Atlassian JIRA.
n. Support the disposition of obsolete and excess IT equipment by sanitizing and preparing equipment for disposal or transfer to appropriate DoD organizations.

C.5.5.3 SUBTASK 5.3 – INCIDENT, PROBLEM, OUTAGE, AND TROUBLE MANAGEMENT

a. The contractor shall notify the DTRA TPOC verbally (or by email if the DTRA TPOC is unavailable) within 15 minutes (or other time period approved by the DTRA TPOC) of confirmation of a mission-system outage.
b. When diagnosing and troubleshooting service outages, the contractor shall escalate to vendor support upon two hours of on-site resolution attempts or sooner upon confirmation of a product or vendor-specific fault that requires vendor response.
c. Coordinate with and follow the direction of Cybersecurity Service Provider (CSP) personnel as directed to address cybersecurity incidents and problems.
d. Monitor the mission support infrastructure and capabilities for emerging and actual incidents, problems, outages, and other events impacting IT performance and/or cybersecurity status.
e. Provide preventative mitigations to faults and service degradations where possible through proactive measures to address service degradation or interruption for DTRA users and mission partners.
f. Provide off-hours remote or call-in support with a two-hour response time for outages to mission capabilities, mission-essential services, infrastructure availability, and DTRA leadership support. Unless otherwise provided in advance, IT capabilities at COOP/DR facilities shall be considered mission-essential services with a four-hour response time to outages of COOP/DR systems when the primary DTRA facility remains functional.
g. Prepare AARs (**Section F, Deliverable 05**) for outages and incidents that degrade or interrupt mission services to users of mission systems and applications. The AAR shall describe the incident, duration, and impact and identify actions taken, potential future preventative actions, and lessons learned.
h. Develop or leverage and update/maintain an online, automated dashboard showing status of infrastructure and system performance, security compliance, and other metrics as

requested by the Government (**Section F, Deliverable 27**).

C.5.5.4 SUBTASK 5.4 – ON-PREMISE SPECIAL PURPOSE PROCESSING NODE (SPPN) OPERATIONS AND MANAGEMENT

The contractor shall perform the following work:

a. Design, manage, operate, and maintain DTRA's Reston SPPN in collaboration with IT engineers and administrators, security personnel, and facilities personnel.
b. Develop, update, and maintain technical, operational, and physical layout documentation and diagrams. (**Section F, Deliverable 29**).
c. Support SPPN designation changes, expansion, migration, and other changes in response to changing DTRA mission requirements and DoD data center architectures.

C.5.5.5 SUBTASK 5.5 – CYBERSECURITY SUPPORT SERVICES

The contractor shall provide cybersecurity services for mission systems and infrastructure in accordance with DoD 8500 series instructions and other applicable DoD and IC publications, instructions, and TOs. The contractor shall also provide security engineering support and guidance to ensure that DTRA mission IT is compliant with all DoD, IC, DISA, and DTRA network security controls, patches, Security Technical Implementation Guides (STIGs), hot fixes, etc. The contractor shall maintain, track, and report contractor personnel certifications under DoDI 8570.01 and subsequent revisions. The contractor shall comply with the direction of DTRA cybersecurity officials, including the AO, SCA, and ISSM.

Contractor IT activities shall comply with DoD and IC cybersecurity implementation guides, instructions, frameworks, and directives. The contractor shall ensure that cybersecurity requirements are treated like other system requirements and are addressed early and continually throughout the IT lifecycle in response to evolving threat, risk, compliance requirements, and mission.

C.5.5.5.1 SUBTASK 5.5.1 – CYBERSECURITY OPERATIONS

The contractor shall ensure that DTRA mission IT enclaves and networks operate in compliance with DTRA enterprise governance and DoD and IC cybersecurity Risk Management Frameworks (RMFs), instructions, and directives (e.g., DoDI 8500.01, DoDI 8510.01, and IC Directive (ICD) 503), cybersecurity warning and TOs, and DISA Computer Network Defense (CND) requirements. CND operations will be staffed on site between the hours of 0800 and 1500 on Government working days. Additional support hours may be required to support incident response, audits, compliance activities, and special events directed by the DTRA TPOC to achieve 24x7 defense of DTRA IT assets.

The contractor shall perform cybersecurity services as required for mission applications, systems, and infrastructure, including:

a. Perform local, on-site cybersecurity operations and defense activities for DTRA MIT enclaves and infrastructure in coordination with the CSP and parent organization cybersecurity functions to prevent, detect, and mitigate intrusions.
b. Provide cybersecurity technical support to patching, remediation, and POA&M activities

for DTRA mission IT infrastructure and production systems.

c. Serve as mission Information Systems Security Officers (ISSOs) as appointed by the ISSM or the Government.
d. Perform security administration, audit log aggregation, and audit analysis within the MIT environment.
e. Administer and maintain anti-virus, anti-malware, host- and network-based security software, filters, rules, devices, and device-level policies in collaboration with network engineers and system administrators.
f. Perform incident response and computer emergency response and support legal investigations and forensic activities.
g. Draft and maintain Cybersecurity Policies and Procedures, Administrative Guides, and Technical Documentation (**Section F, Deliverable 44**).
h. Provide mission IT-related security engineering and design guidance support throughout the SDLC.
i. Provide technical briefings and support to security-operations-related meetings with DTRA leadership.
j. Provide management of DTRA Public Key Infrastructure (PKI) hardware, user authentication tokens, and certificates (e.g., SIPRNet CACs, soft or digital certificates, etc.). Issue, revoke, replace, and manage on-site operations and inventory for authentication tokens and pin resets. The contractor shall maintain a DISA-compliant registration authority and issue SIPRNet CACs on site between the hours of 0800 and 1700 on Government workdays.
k. Provide periodic manual and automated data transfer services including cross-domain file transfers, scans, and reviews in response to user requests and Government direction.
l. Provide liaisons and coordinate incident responses with the DoD and IC cybersecurity authorities, DTRA’s Cybersecurity Service Provider (CSSP), and other similar organizations.
m. Support DTRA Emissions Security (EmSec) and physical security efforts, including coordination with physical security personnel where appropriate.
n. Maintain a current list of authorized privileged users, manage authorization and revocation of privileged users, and ensure least privilege of user accounts and user awareness of security responsibilities (**Section F, Deliverable 45**).
o. Review and update DTRA user agreements to maintain compliance with evolving DoD and IC requirements **(Section F, Deliverable 46)**.
p. Support Government efforts for preparation, engagement, and successful outcome of DoD and IC cybersecurity inspections and tests.

C.5.5.5.2 SUBTASK 5.5.2 – CYBERSECURITY AND RISK MANAGEMENT SUPPORT

The contractor shall provide DoD and IC Risk Management Framework (RMF) support locally for mission applications, systems, and infrastructure in compliance with DTRA risk management governance including authorizations, risk assessments, and threat assessments. The contractor shall draft and staff authorization packages, authorization letters, and other risk management documentation for all DTRA IT assets (e.g., infrastructure, networks, interconnections, commercial software, custom developed applications, systems, and frameworks).

The contractor shall perform security services throughout the mission system lifecycle, including:

a. Ensure that risk management packages are developed and maintained concurrently throughout the system life cycle, beginning at inception of new IT activities.
b. Comply with and coordinate with DTRA CM processes.
c. Support DTRA cybersecurity and risk management officials including the Authorizing Official (AO), Information Security Systems Manager (ISSM)(s), and Security Control Assessor (SCA).
d. Execute risk management support and develop packages using processes and templates that are approved by the cognizant risk management official.
e. Support DTRA's implementation of the DevSecOps path to production and support implementation of automated testing and validation capabilities in collaboration with software developers as required.

The contractor shall perform risk management support services as directed by the Government:

a. Support DTRA's efforts to implement and comply with DoD and IC RMF authorization processes.
b. Maintain and populate DTRA's instance of the DoD Enterprise Mission Assurance Support Service (eMASS) for mission systems and infrastructure.
c. Prepare and maintain RMF packages, including security plans, system descriptions, diagrams, data flows, POA&M, security assessment reports, and other documentation (**Section F, Deliverable 47**).
d. Provide technical support to risk assessments and risk determinations, including preparation of Cybersecurity Impact Assessments (**Section F, Deliverable 48**) that summarize test results, risks, and threats in support of ISSM, SCA, and AO risk decisions.
e. Ensure that preparation of RMF and other cybersecurity materials (**Section F, Deliverable 47**) are complete and delivered for Government risk reviews and decisions NLT 30 calendar days prior to the applicable authorization decision date.
f. Provide security engineering support throughout RMF IT life cycles in coordination with system engineers and software developers. Examples include identification of common controls, system categorization, security control selection, and security control tailoring and providing design and implementation guidance to software developers, system engineers, and network engineers.
g. Review IT system plans, designs, configurations, and architectures for compliance with DoD cybersecurity requirements.
h. Assist Government cybersecurity officials with design and implementation of RMF workflow, processes, and procedures.
i. Maintain appropriate, current computing environment, and cybersecurity certifications and obtain appointment letters (e.g., ISSO, Privileged Users, etc.) signed by DTRA cybersecurity officials.

j. Provide coordination, liaison, and support of cybersecurity-related relationships with external partner organizations, including preparation of cybersecurity-related documentation and agreements for interconnections, reciprocity, and DTRA DR and COOP facilities.
k. Assist the Government with drafting and maintaining Cybersecurity Policies and Procedures (**Section F, Deliverable 44**).
l. Support the Government's risk management and approval of commercial, third-party, and open-source software.
m. Provide technical briefings, meeting support, and status updates related to cybersecurity and risk management (**Section F, Deliverable 12**).

C.5.5.5.3 SUBTASK 5.5.3 – COMMUNICATIONS SECURITY (COMSEC)

The contractor shall provide a certified COMSEC manager and alternate. The contractor shall acquire, integrate, and test COMSEC equipment and handle COMSEC keys in accordance with Government (i.e., the National Security Agency) COMSEC and key management directives. Support is required to include accountability, issue, operation, destruction, and turn in of all COMSEC key material and equipment and support of re-key operations. The contractor shall identify, report, and support any changes in DTRA's COMSEC account that may result from to transition to DTRA.

The contractor shall:

a. Perform as a COMSEC POC, track all actions involving COMSEC management and support the maintenance of COMSEC accounting records.
b. Prepare reports concerning COMSEC incidents in accordance Government regulations and COMSEC Maintenance Forms, Logs, and Reports pertaining to COMSEC material accountability (**Section F, Deliverable 49**).
c. Maintain up-to-date knowledge of the use the Key Management Systems (KMS) and specialized hardware and software programs used to generate and maintain COMSEC material.
d. Handle daily operational matters based on knowledge of COMSEC management and use that knowledge to refer inquiries to appropriate personnel.
e. Provide support on COMSEC matters pertaining to the use of secure communications devices.
f. Maintain cryptologic equipment in operational condition and coordinate with DTRA IT engineers to address outages resulting from equipment failure, failed re-key transactions, and other issues that can affect network and system availability.
g. Support COMSEC audits and inspections by cognizant Government oversight authorities.

C.5.5.6 SUBTASK 5.6 – PROVIDE ASSESSMENT AND TESTING SERVICES

The contractor shall ensure that DTRA mission capabilities, infrastructure, systems, and applications are tested in compliance with DTRA, DoD, and IC instructions, directives, frameworks, and standards. The contractor shall support design and implementation of advanced or automated testing capabilities to accelerate delivery of mission capabilities. The contractor shall provide DTRA Government leads with accurate, objective, and impartial verification of the compliance status of mission applications, systems, and infrastructure. The contractor shall ensure that DTRA testing activities are coordinated, planned, and executed as part of IT system lifecycles and projects. The contractor shall provide effective capacity planning and reporting to enable the DTRA TPOC to prioritize tasks and focus testing resources on critical DTRA priorities. The test team shall track and report information such as test capacity, queues, priorities, completion status, performance statistics, and schedules by creating or leveraging a portal or other automated reporting capability approved by the Government (**Section F, Deliverable 27**).

C.5.5.6.1 SUBTASK 5.6.1 – PREPARE/MAINTAIN SECURITY ASSESSMENT PLANS AND TEST PLANS

The contractor shall prepare and maintain Assessment and Test Plans (**Section F, Deliverable 50**), as directed by the Government. The assessment and test plans shall describe the methodology by which the contractor shall execute each type of testing and shall contain information as requested and approved by the SCA and DTRA TPOC. The contractor shall propose efficient methods of maintaining test plans to minimize paperwork and cost.

C.5.5.6.2 SUBTASK 5.6.2 – DEVELOP TEST PROCEDURES

The contractor shall develop or identify Test Procedures and Test Cases (**Section F, Deliverable 51**) for each new DTRA software application, widget, system, integration effort, or technology insertion into the mission enclave as requested by the Government. Test procedures shall be in compliance with DoD and IC directives, frameworks, and guides (e.g., DoDI 8500 series, DISA STIGs, or Security Requirements Guides) The contractor shall leverage test procedures, security control assessment procedures, and test tools provided or mandated by the DoD, IC, or other Government entity. This includes continuous monitoring methods in compliance with DoD and DTRA direction. When pre-defined test procedures are not available, the contractor shall propose test procedures for SCA approval and for inclusion in the security assessment report. The contractor shall continuously manage and optimize test methodologies and approaches to improve efficiency and reduce costs.

C.5.5.6.3 SUBTASK 5.6.3 – CONDUCT ASSESSMENT AND TESTING ACTIVITIES

The contractor shall execute approved test procedures to validate the implementation of cybersecurity controls and requirements for DTRA MIT assets. Testing shall be conducted to support authorizations, re-authorizations, periodic network tests/scans, periodic compliance testing, continuous monitoring, and preparation for readiness inspections and audits as directed. The contractor shall re-test or validate bug fixes and other remediation activities identified in previously completed test activities.

The contractor shall conduct security control assessments in compliance with DoD and IC cybersecurity instructions and RMFs. The contractor shall apply, where feasible, test procedures, methodologies, and tools identified by the DoD and the IC (e.g., DoDI 8500 series, DISA STIGs, DISA Security Requirements Guides (SRGs), and DoD's Knowledge Service). The contractor shall support DTRA continuous monitoring and periodic security control assessments. The contractor shall perform testing of cross-domain solutions using approved test plans in coordination with cybersecurity operations personnel.

The contractor shall review and assess software code, review software code scans and assessment reports, and operate software code scanning tools as prescribed by DoD RMFs and technical guides. The contractor shall identify the existence and causes (where feasible) of deficiencies, vulnerabilities, and other findings within software code.

The contractor shall design, implement, and maintain a test environment on each level of network as directed by the DTRA TPOC and in coordination with the SCA or other Government testing authority. The test environment will be populated with Government-Furnished Equipment (GFE). The contractor shall prepare and update as, as directed by the Government, a Test Environment Design and Management Plan, Master Test Plan (**Section F, Deliverable 30).**This plan shall contain information such as the design or architecture of the test environments, required tools, hardware, software, administrative procedures, and the contractor's approach to maintaining test environments.

C.5.5.6.4 SUBTASK 5.6.4 – PREPARE ASSESSMENT AND TEST REPORTS

The contractor shall prepare reports that capture all tests/assessments and results with content and structure as approved by the SCA and/or the DTRA TPOC (**Section F, Deliverable 50**). Where feasible, the reports will include technical recommendations for remediation or mitigation of deficiencies. Reports shall include descriptions of deficiencies and their severity to enable risk determinations by the SCA or other personnel. The contractor shall deliver test reports to Government and industry personnel as required. The contractor shall provide technical input to the development of POA&Ms, risk assessment activities, remediation planning, and bug-fix planning. The contractor shall, where feasible, leverage automated test reports or the output of automated tools to improve efficiency and minimize paperwork.

Test reports and artifacts shall be prepared as an addendum to or component of risk management packages, security assessment reports, authorization letters, memoranda, or other documentation packages. Artifacts may include output from automated test tools, code scan reports, screen shots that depict aspects of system configuration, and other information requested by Government risk management officials.

C.5.5.7 SUBTASK 5.7 – PROVIDE DEPLOYED IT CAPABILITIES

The contractor shall provide robust, flexible, secure, and sustained deployed IT capabilities to DTRA and its mission partners. The contractor shall provide 24x7 phone response and remote support to deployed users of DTRA expeditionary capabilities. The contractor shall tailor capabilities to meet the unique mission requirements identified by the Government and shall provide logistical support to ensure that capabilities are delivered by the mission-requirement date. The contractor shall support continuous improvement and identify efficiencies for improved capabilities for deployed users. The contractor shall maintain proficiency with deployed IT capabilities and knowledge of each system's configuration sufficient to provide step-by-step remote assistance to deployed users for all aspects of system assembly, connection, operation, problem resolution, and disassembly.

Deployed IT capabilities include DTRA expeditionary kits and other capabilities that may be tailored to mission-partner or emerging requirements (e.g., lightweight kits, specialized communications, or computing gear). Deployed IT capabilities are an extension of the DTRA mission infrastructure that provide a remote, self-contained desktop, mission IT analytical tool suite, and communications equipment to deployed analysts. Deployed IT capabilities are designed to operate in austere, remote locations with minimal or no local IT support. These capabilities generally consist of a standardized platform and suite of communications and analytical software tools that are customized to meet the requirements of each operational location and mission partners. Contractors shall determine the necessary components and design to enable deployed capabilities, which will then be purchased by the Government. This may include, but not limited to, these types of equipment: ruggedized laptops, satellite data and voice equipment, modems, monitors, mobile or satellite phones, encryption, peripherals, external hard drives, token readers, switches, hubs, transceivers, backpacks, commercial and Government software suites, shipping containers, spare parts, and miscellaneous items (**Section J, Attachment K**).

C.5.5.7.1 SUBTASK 5.7.1 – DEPLOYED INFORMATION TECHNOLOGY (IT) CAPABILITY INTEGRATION

The contractor shall provide support including assembly, integration, O&M, pre-deployment training, logistics, shipping, and Tier II and III technical support and remote user support. The contractor shall track and report status and location of all Deployed IT capabilities and associated equipment. The contractor shall provide complete Deployed IT capabilities life-cycle management, maintain bench stock and spare parts for repairs and kit refurbishment, and manage life-cycle replacements for aging or damaged kits.

The contractor shall provide the following Deployed IT capability life-cycle support including, but not limited to:

a. Assess IT infrastructure, mission, operational, communications requirements, and unique TTPs for each deployed IT capability deployment location.
b. Assess operational readiness and mission worthiness of each deployed IT capability.
c. Identify and implement, with Government approval, options to mitigate the risk of equipment failure upon deployment.
d. Identify necessary equipment, telecommunications, encryption, and bandwidth requirements and providing cost estimates where required.
e. Follow DTRA CM procedures, prepare Configuration Review Board (CRB) Requests, (**Section F, Deliverable 52**), and provide technical support to Government approval processes.
f. Integrate all equipment and telecommunications capabilities required to support the mission at the target location. Deployed IT capabilities are built on standard DTRA device images to ensure compatibility and ease of O&M.
g. Collaboration of communication services, tracking and supporting provisioning of expeditionary kit communication services to include directed sources such as DISA.
h. Support RMF activities in collaboration with DTRA cybersecurity and IT personnel to ensure deployed IT capability compliance, approved software images, and authorizations to operate and connect to DTRA enclaves.
i. Provide design and other documentation (**Section F, Deliverable 29**) necessary to obtain authorization to operate and connect Deployed IT Capabilities to Government networks.

C.5.5.7.2 SUBTASK 5.7.2 – TECHNICAL AND LOGISTICS SUPPORT FOR DEPLOYED INFORMATION TECHNOLOGY (IT) CAPABILITIES

The contractor shall perform the following logistics services including, but not limited to:

a. Prepare a Pre/Post Logistics Plan (**Section F, Deliverable 53**), subject to Government approval, for each Deployed IT capability to be deployed.
b. Conduct pre-deployment receipt and inspection of all IT equipment, documentation, shipping containers, and other material that will be deployed in support of the DTRA analytical teams.
c. Perform pre-deployment staging and testing of the DTRA expeditionary kit and upgrades, including conduct a complete inventory of assets being deployed, replenish missing items, interconnect equipment, and run test procedures to ensure the DTRA expeditionary kit or upgrade is functional and meets approved contractor-proposed exit criteria and checklists before shipping.
d. Provide secure/survivable packaging, handling, shipping, transportation, and logistics to deliver deployed IT capabilities to approved destinations.
e. Provide remote, reach-back technical support for in-theater receipt, inspection, set-up, and disassembly to ensure the deployed IT capability is functional and meets approved acceptance criteria. In-theater support may be required upon Government approval of Temporary Duty (TDY).
f. Document all deployed IT capability hardware by creating hand receipts and following property control procedures required by DTRA and DTRA’s mission partners.
g. Provide Tier II and Tier III Government-site user technical support from 8 a.m. to 5 p.m. Monday through Friday, excluding Government holidays. The contractor shall provide on-call phone support for infrastructure related issues after hours to deployed users in remote locations, including users operating in potentially austere or hazardous conditions with no local IT or communications support. The contractor shall maintain proficiency with deployed IT capabilities and knowledge of each system’s configuration, sufficient to provide step-by-step remote assistance with all aspects of system assembly, connection, operation, and disassembly.
h. Collaborate with DTRA watch operations to enable a fully integrated and coordinated user support experience that is easily accessible 24x7 for users of deployed IT capabilities.
i. Provide Capability Status Reports (e.g., operational readiness, deployment location, shipping status, functional capabilities, and training schedules), inventory, purchase plans, technology roadmaps, and other information to support DTRA mission leadership (**Section F, Deliverable 54**).

C.5.5.7.3 SUBTASK 5.7.3 – DTRA EXPEDITIONARY KIT TRAINING

The contractor shall provide hands-on, system-specific training to familiarize users with the assembly, operation, disassembly, and inventory control of deployed IT capabilities. The objective of training is to maximize the effectiveness of DTRA’s support to the warfighter and to reduce end-user dependence on reach-back support while in remote operating areas. The contractor shall develop and provide training materials, electronic and hard-copy user guides, reach-back support instructions, and other materials to meet mission requirements (**Section F Deliverable 40**).

C.5.5.7.4 SUBTASK 5.7.4 – TELECOMMUNICATIONS, SATELLITE, AND MICROWAVE LINE-OF-SIGHT ENGINEERING SUPPORT

In support of DTRA deployed IT capabilities, the contractor shall procure, design, integrate, support, and maintain wireless, microwave, and satellite and communications capabilities in response to mission requirements. For example, the contractor shall integrate and maintain mobile/portable satellite communications systems to ensure that deployed IT capabilities are self-contained to support deployed forces operating in austere locations. The contractor shall provide telecommunications user support and reach-back capabilities. As directed by the Government, the contractor shall acquire satellite communications services.

The contractor shall provide a DTRA Deployed IT Telecommunications and Satellite Requirements Report (**Section F, Deliverable 55**) which includes cost and functional analysis, assessments, risks, and courses of action to meet deployed or mobile user telecommunication requirements.

C.5.5.8 SUBTASK 5.8 – MISSION APPLICATIONS AND SYSTEMS SERVICE DESK

The contractor shall staff service desk on-site in DTRA facilities to support DTRA mission applications and systems, as defined in the scope of this TO (e.g. MIT applications, systems, infrastructure, etc.). The service desk is currently located in DTRA’s Reston, Virginia, facility and shall operate 24x7 with full staffing between the hours of 6 a.m. and 10 p.m. on workdays. The service desk shall operate with reduced mission system support staffing from 10 p.m. to 6 a.m. and on Government holidays to maintain mission support and ability to respond to DTRA mission partners who operate in other time zones or on a 24x7 schedule. The contractor is not required to provide on-site staffing of the service desk during unplanned closures of the Government facility (e.g., weather closures, etc.).

The contractor shall provide as-needed 24x7 remote technical phone support and four-hour response times, as directed by the DTRA TPOC, to deliver on-site support for resolution of outages and performance degradation of critical mission systems during non-business hours. Four-hour response times shall include infrastructure, software development, cybersecurity, and system integration support.

Increases or reductions in service desk hours of operation, services, and/or LOE including elimination of local service desk support and transfer to an enterprise provider may be implemented after coordination among the contractor, FEDSIM COR, and DTRA TPOC. For example, adjustments may be required in support of emerging DTRA mission requirements, organizational changes, mission partner requests for support, or DTRA transition activities. Response to these requirements may result in permanent or limited-duration changes to service desk support.

The service desk shall serve as the single, initial contact point for mission system users to resolve incidents and problems, including mission IT capabilities, cybersecurity, hardware, software, networks, telecommunications, and connectivity for all mission infrastructure.

Work activity may include some or all of the following activities.

The contractor shall support the following activities, including but not limited to:

a. Open incident tickets, verify accuracy, and resolve the problem, or forward the problem to the appropriate technical support staff in accordance with performance measures and AQLs identified in the PRS/SLAs (**Section J, Attachment F**).
b. Monitor, manage, and optimize user call queues and responses to service-desk phone calls.
c. Utilize remote support tools such as DTRA's implementation of Bomgar to the maximum extent practicable. Provide touch labor when required.
d. Escalate resolution of an incidents according to DTRA approved escalation procedures.
e. Provide daily ticket queues and Very Important Person (VIP) support status to Government customer service leads via dashboard, email updates, and in person where required.
f. Establish and maintain accounts and passwords for mission-system applications and systems users.
g. Obtain a customer satisfaction report for each incident, IAW PRS/SLA requirements (**Section J, Attachment F**), periodically survey users for overall satisfaction, and support third-party or independent user surveys and quality assessments.
h. Coordinate incidents with the DoD or DTRA enterprise service provider as required to resolve mission IT incidents and problems.
i. Assess the existing self-help capability and improve or re-develop and maintain an automated, on-line, easily accessible, user self-help feature, including a Frequently Asked Questions (FAQ) list, with the intent of reducing the need for users of mission capabilities to contact the Service Desk (**Section F, Deliverable 56**).